CS50: Proof - Sudoku Solutions

Irene Lam, Kelly Westkaemper, David Kantor, David Perez Gonzalez

August 27 2020

1 Introduction

The over-arching mathematics behind this proof is rooted in Group Theory and understanding certain important properties of groups. Lets begin with some basic definitions.

1.1 Definition

Set: A set is a collection of distinct well defined objects.
Group: A group is a set and an operation that respects 3 basic axioms: associative, closed under the operation, inverse element must exist, and the identity element exist.
Group Homomorphism: Given two groups G and H there is a mapping that exists between G and H that respects the algebraic structure of G in H. In order for a mapping to be a group homomorphism:

$$f(a * b) = f(a) * f(b) \quad \forall a, b \in G \tag{1}$$

Injective: If for every element x in the codomain X of the function there is one element such that f(a) = x for an element a in the domain A then the function is said to be injective from A to X.
Surjective: IF for every element in the codomain there is at least one element that the function maps from the domain and hits every element in the codomain then the function is said to be sujective.
Group Isomorphism: If a group homomorphism is both surjective and injective then it is bijective. A bijective group homomorphism is called an isomorphism and it is a function mapping that completely respects the algebraic stucture between groups.

2 Proposition

The proposition we will be tackling this proof is that we can generate and guarantee a unique Sudoku puzzle solution given certain parameters. We will be using Group Theory to generate a homomorphism between two groups and then take advantage of relabeling and reorganization to generate valid sudokus with only one possible solution

3 Proof

Let us start this proof by looking at one of the most obvious groups

$$Z_3$$

. This group consists of the elements 0,1,2. From here we can then take a look at the product group of

$$Z_3 \ x \ Z_3 \tag{2}$$

The elements of this group are defined as:

$$Z_3 \ x \ Z_3 := \{(a, b) : a \in Z_3, b \in Z_3\} \tag{3}$$

We can take a look at the Caley table of this group which looks like (wikipedia):

Grid 1 – The addition table in $\mathbb{Z}_3 \oplus \mathbb{Z}_3$

(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)	(2,0)	(2,1)	(2,2)
(0,1)	(0,2)	(0,0)	(1,1)	(1,2)	(1,0)	(2,1)	(2,2)	(2,0)
(0,2)	(0,0)	(0,1)	(1,2)	(1,0)	(1,1)	(2,2)	(2,0)	(2,1)
(1,0)	(1,1)	(1,2)	(2,0)	(2,1)	(2,2)	(0,0)	(0,1)	(0,2)
(1,1)	(1,2)	(1,0)	(2,1)	(2,2)	(2,0)	(0,1)	(0,2)	(0,0)
(1,2)	(1,0)	(1,1)	(2,2)	(2,0)	(2,1)	(0,2)	(0,0)	(0,1)
(2,0)	(2,1)	(2,2)	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(2,1)	(2,2)	(2,0)	(0,1)	(0,2)	(0,0)	(1,1)	(1,2)	(1,0)
(2,2)	(2,0)	(2,1)	(0,2)	(0,0)	(0,1)	(1,2)	(1,0)	(1,1)

The group operation in this table is addition modulo 3 and thus combine all the elements in this form we see the caley table represent above.
Next from the Fundamental Homomorphism Theorem we know that there must exist a group homomorphism that maps:

$$Z_3 \; x \; Z_3/ker(\pi) \cong Z_3 \tag{4}$$

One way to interpret the previous equation is that we want to show this group is isomorphic to quotient subgroup namely the integers mod 3, that allows us to preserve the group structure. Shifting focus for a second let us prove why the caley table above has the property that no row or columns contains an entry of repetition.

3.0.1 Mini-Proof

Proposition: Prove that we can never have a finite group G under an operation *, have the operation table contain more than one element in every row and column.

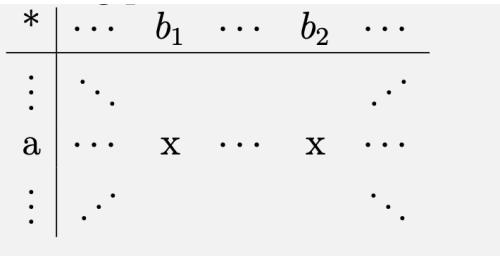

Figure 2: Show why we cant have this picture for any row or column

Proof:
They both share a very similar logic so we will show the reasoning for rows and the proof for columns is very similar. If we assume that an element x is repeated in a row then going off of the property of the group equation then a*b has two solutions for any element a,b ∈ G. If we then assume b_1 and b_2 to be solutions to this equation, we derive:

$$a * b_1 = x \qquad a * b_2 = x \tag{5}$$

$$a * b_1 = a * b_2 \tag{6}$$

$$b_1 = b_2 \tag{7}$$

We can multiply by a^{-1} on both sides since we know a to have an inverse and be closed under operations since it is an element of the group G. Thus we have arrived that our assumption of two different solutions is in fact only one distinct solution, and why we have a unique element in each row.
Now going back to the original proof let us define a group homomorphism π as the following:

$$\pi : Z_3 \; x \; Z_3 \longrightarrow Z_3 \tag{8}$$

$$\pi((a, b)) = a \tag{9}$$

Let us prove that this is infact a group homomorphism

$$\pi((a, b) + (c, d)) = \pi((a + c, b + d)) = a + c = \pi((a, b)) + \pi((c, d)) \tag{10}$$

Let us check that this function is injective and surjective:

$$\pi((a, b)) = \pi(c, d) \tag{11}$$

This homomorphism is injective because in order for equation 11 to be true under this function rule then a =c and thus proving a 1 to 1 mapping. Next let us check surjectivity:

$$\pi((a, 0)) = a, \quad \forall a \in Z_3 \tag{12}$$

Thus we have shown this function is surjective and injective and therefore bijective and by definition this homormorphism is isomorphic thus the quotient ring Z_3 respects the same group structure as the cross group and thus we can rearrange the entries such that the entries arent repeated within a 3 by 3 grid thanks to this homomorphism and we can then simply relabel each point as a number 1-9 and generate a valid sudoku with a unique solution. We can also use short exact sequences (outside scope of this proof) to show that you can even generate sudokus using groups that aren't the same size. Those would look something like the form:

$$Z_M \longrightarrow Z_M \; x \; Z_N \longrightarrow Z_N \tag{13}$$

Using this method we can genearate around 3 million possible sudoku puzzles each with a unique result. The total number possible unique sudoku puzzle gneerated was computer in 2005 by Felgenhaver and Jarvis